IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method of providing secure access to content comprising:

determining a secure medium identification (disk ID) from a secure medium including content, wherein the content is stored as encrypted content on the secure medium;

sending [[a]] an encrypted one-time session key and the disk ID to a server;

requesting user authentication; ~~and~~

if the user is successfully authenticated, receiving a ~~decrypted~~ copy of the encrypted one-time session key from the server to enable reading of the content on the secure medium;

receiving a content decryption key from the server, in response to the disk ID and the user authentication, wherein the content decryption key is determined based on the disk ID;

using the content decryption key and the session key returned by the server to decrypt the content received from the secure medium; and

playing the decrypted content.

2. (Previously Presented) The method of claim 1, further comprising:

streaming encrypted content from the secure medium to an application.

3. (Previously Presented) The method of claim 2, wherein the application uses the one-time session key returned by the server to decrypt the encrypted content, and display the decrypted content.

4-7. (Canceled)

8. (Currently Amended) The method of claim 1, further comprising a operating trusted device for accessing secure content:

reading the disk ID from the secure medium and generating the one-time session key; and

sending an encrypted copy of the disk ID and the one-time session key to the server.

9. (Previously Presented) The method of claim 8, wherein the disk ID and one-time session key are encrypted using a symmetric key.

10. (Previously Presented) The method of claim 1, wherein the secure medium is selected from among the following: an optical disc, a flash memory, a hard drive, a magnetic drive, a memory stick, or a storage device to store encrypted content.

11. (Original) The method of claim 1, wherein the content is digitally encoded music.

12. (Original) The method of claim 1, wherein user authentication comprises one or more of the following: a credit card, a debit card, electronic cash, a user-specific ID card.

13. (Original) The method of claim 1, wherein the user authentication comprises one or more of the following: a password, a user identification, a biometric identification.

14-16. (Canceled)

17. (Currently Amended) An apparatus comprising a secure device for accessing secure content coupled to a client system comprising:

a reader to read an identification (ID) and content from a secure medium;

a session key generation logic to generate a one-time session key;

an encryption logic to send the ID and the session key encrypted to a server;

an authentication logic to receive authentication from the server indicating approval to read the content of the secure medium;

the reader further to pass the ID and the content to the encryption logic; ~~and~~

the encryption logic further to encrypt the content prior to sending the content to an application; and

an application on the client system, the application comprising:

a user authentication interface to request a user authentication in response to a server request, and to send data received from a user to the server;

a key logic to receive a decryption key from the server, if the user is successfully authenticated, wherein the decryption key includes both the session key and a content decryption key; and

a streaming decryption logic to receive content from the secure device and to decrypt the content using the decryption key received from the server, and to play the content.

18. (Original) The apparatus of claim 17, wherein the encryption logic uses a symmetric key to encrypt the ID.

19-21. (Canceled)

22. (Previously Presented) The apparatus of claim 17, further comprising a secure server coupled to the client system via a network, the secure server comprising:

a network interface to receive the ID and the session key from the secure device;

a user validation logic to request a user validation from the client system and determine whether the user has permission to access the secure medium identified by the ID; and

an encryption logic to return the session key and a content decryption key to the client system if the user has permission to access the secure medium.

23. (Original) The apparatus of claim 22, further comprising:

the encryption logic further to decrypt data received from the secure device using a symmetric key.

24. (Original) The apparatus of claim 22, further comprising:

an ID lookup to determine the content decryption key based on the ID.

25. (Previously Presented) A client system to securely access digital content on a secure medium, the client system comprising:

a secure device comprising:

a reader to read a disk identification (disk ID) and content from the secure medium;

an authentication logic to receive authentication from a server indicating approval to read the content of the secure medium; and

an encryption logic further to encrypt the content prior to sending the content to an application;

the application comprising:

a user authentication interface to request a user authentication in response to a server request, and to send user authentication data received from a user to the server;

an association logic to determine if the disk ID is associated with the user, and;

if the disk ID is not yet associated with the user, to associate the user authentication data with the disk ID; and

if the disk ID is associated with the user, determining that the current user authentication matches the user associated with the disk ID, to authenticate the user;

a key logic to receive a decryption key from the server, if the user is successfully authenticated; and

a streaming decryption logic to receive encrypted content from the secure device and decrypt the encrypted content using the key received from the server, and play the decrypted content.

26. (Previously Presented) The client system of claim 25, further comprising: a session key generation logic to generate a one-time session key, the session key sent with the ID to the application.

27. (New) A method of providing secure access to content, the method comprising:

determining a secure medium identification (disk ID) from a secure medium including content;

sending an encrypted one-time session key and the disk ID to a server;

requesting user authentication, wherein user authentication comprises:

determining if the disk ID is already associated with a user, and

if the disk ID is not yet associated with the user, associating the user authentication data with the disk ID; and

if the disk ID is associated with the user, determining that the user authentication matches the user associated with the disk ID, to authenticate the user;

if the user is successfully authenticated, receiving a copy of the encrypted one-time session key from the server to enable reading of the content on the secure medium; and

wherein if the user authentication does not match the user associated with the disk ID, the session key is not received from the server, preventing display of the content.